(19) Eur päisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 939 571 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.09.1999 Bulletin 1999/35

(51) Int. Cl.[6]: **H04Q 11/00**

(21) Application number: **98103449.9**

(22) Date of filing: **27.02.1998**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant:
TELEFONAKTIEBOLAGET L M ERICSSON (publ)
126 25 Stockholm (SE)

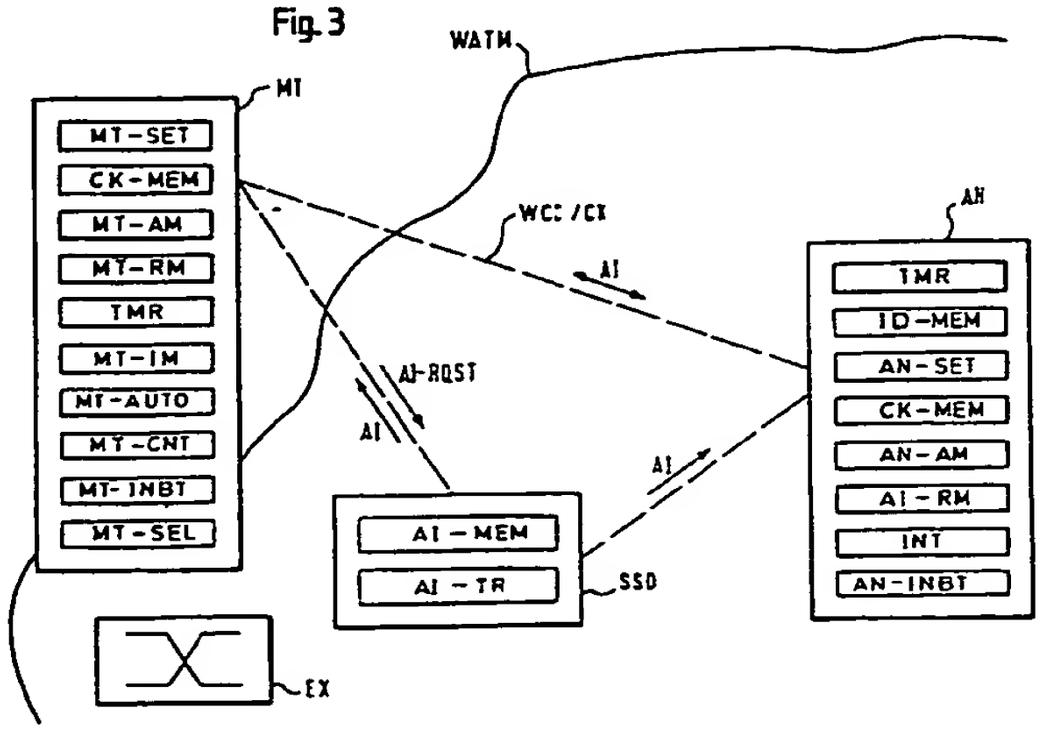
(72) Inventors:
- **Keller, Ralf**
  52146 Würselen (DE)
- **Wrona, Konrad**
  52134 Herzogenrath (DE)

(74) Representative:
Ritter und Edler von Fischern, Bernhard, Dipl.-Ing. et al
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Authentication method and authentication device for secured communications between an ATM mobile terminal and an ATM access node of a wireless ATM radio communication network

(57) A mobile terminal (MT) sets up a wireless ATM radio communication connection (WCC) to an access node (AN) of a wireless ATM radio communication network (WATM). On the communication connection (WCC) a secret communication key (CK) is used which has been agreed upon by the ATM access node (AN) nd the ATM mobile terminal (MT). Once the operating communication connection (WCC) is established, the mobile terminal (MT) can request authentication information (AI) from the security server (SSD) located in the (WATM) system or another network (FN) connected to the access node (AN). If after setting up the communication connection (WCC) the authentication information (AI) is received in a predetermined time period at said access node (AN) , the mobile terminal is authenticated at the access node (AN). Since the communication channel (WCC) is always setup before the authentication procedure, also security functions from other interconnected networks can be accessed and thus a high level of confidentiality as well as security can be maintained.

Fig. 3



EP 0 939 571 A1

Printed by Xerox (UK) Business Services
2.16.7/3.6

Description

Field of the Invention

[0001] The invention relates to a method for setting up a secured communication between an ATM mobile terminal and an ATM access node of a wireless ATM radio communication network. Furthermore, the invention relates to an authentication device for such a wireless ATM radio communication network. The invention also relates to the ATM access node of such a wireless ATM radio communication network. Furthermore, the invention relates to an ATM mobile terminal usable within such a wireless ATM radio communication network.

[0002] In wireless ATM radio communication networks, generally two steps must be performed in order to connect an ATM mobile terminal to an ATM access node, namely an authentication step where authentication information is exchanged between the mobile terminal and the access node, and a second step in which the wireless connection is set up and in which a secret ciphering key is agreed upon (which is used in an encryption procedure to encrypt the data to be transmitted) such that the wireless ATM connection has a high degree of confidentiality. The exchange of authentication information and the setting up of the wireless connection with the agreed confidentiality key requires the exchange of signals between the mobile terminal and the access node according to a predefined protocol.

[0003] Some protocols allow the exchange of the shared authentication information prior to setting up the wireless connection with the session key. However, as will be explained below, there are some protocols a session needs to be first established and only then the secret shared authentication information can be made available. This drawback is very significant, if for example a first signaling protocol is used on the wireless link between the mobile terminal and the access node and another protocol is used between the access node of the ATM communication network and an access node of other interconnected fixed networks.

[0004] The invention in particular relates to the establishment of a secure ATM wireless connection between the ATM mobile terminal and the ATM access node for the case where different signaling protocols are used.

Background of the invention

[0005] Wireless ATM systems are currently standardized within both the ETSI project BRAN and the ATM Forum Wireless ATM group. Examples of such wireless ATM systems are for example an ATM wireless access communication system (AWACS system), a wireless professional and residential multimedia applications (MEDIAN application) for indoor customer premises networks, the Magic WAND demonstrator (wireless ATM network demonstrator) for indoor and outdoor applications in customer premises and public networks, the SAMBA system, an ATM based mobile system like a broadband mobile communication for multimedia on ATM-basis supported by the German Ministry for Research and Education, or a high performance radio local area network (HIPERLAN system) etc.

[0006] Each of the aforementioned wireless ATM systems is defined for specific different application areas. Some of them are for example designed for wireless local area networks (LANs) or to the extension or replacement of fixed LANs. Other systems are specifically designed for broadband access (e.g. to UMTS or to the GSM or GPRS core networks) or to point-to-multipoint systems.

[0007] A general configuration of interacting networks including wireless ATM systems is shown in the attached Fig. 1a. Such systems are currently investigated in the aforementioned standardizing committees. As is seen in Fig. 1a, several different types of networks are interconnected through access nodes AN (also called access points). The network A may be provided for fixed wireless components communicating through a wireless channel (e.g. through fixed wireless LANs and a network access via microwave links). The network B may comprise mobile end users communicating directly with the fixed network switching elements (e.g. digital cellular telephony, PCS, wireless LAN). The networks C, D may represent mobile switches with fixed end users where the end users have a fixed connection (either wired or wireless) to a switch. The switch and the end user, as a unit, are mobile, with the switch having a wired or wireless connection to fixed network switching elements (e.g. to a fixed network on board of a passenger plane, military aircraft or navel vessel). Furthermore, in the network D mobile switches with mobile end users may be provided, i.e. the mobile terminals establish connections with switches which are themselves mobile and which then establish a connection to a fixed network, as is the case e.g. in LEO satellite based switching to mobile stations, wireless end user devices; wireless connection to mobile switches on emergency or military vehicles). Another example is shown at E, which is summarized as wireless ad hoc networks. Here, wireless networks are provided, when there is no access node available (e.g. laptops gathered together in a business conferencing environment). It also considers cases where access nodes cannot be placed at arbitrary locations and where plug-and-play and network flexibility are important considerations (e.g. for a residential user). This requirement can be met by supporting auto-configuration of a wireless ATM network. Both mobile end users and fixed wireless end users are possible. Ad hoc networks can also extend the coverage of existing access-node-orientated networks by wireless means by use of forwarding nodes, which act as intermediate relay points (transfer nodes) and forward ATM packets from one WATM radio frequency to another WATM radio frequency. It is envisaged that in the initial stage a wireless ATM system will use an operating fre-

quency of 5 GHz and a available user data rate of 25 Mbit/s. The estimated cell range will be between 30 - 50 m indoors and 200 - 300 m outdoors.

[0008] As shown in Fig. 1a, there are various possibilities how mobile ATM (asynchronous transmission mode) networks may be interconnected through the access nodes AN and, since the communication connections are ATM connections and are wireless, the security aspect is an important consideration in such a network architecture. In particular, the interoperability with security mechanisms of other networks is an important aspect. Also simplicity of upgrading and adding new functionalities is very important, especially as it is impossible to prove that any of the existing practical cryptosystems cannot be broken in future, due to the progress in mathematical theory and development of new more efficient algorithms.

[0009] Therefore, as explained above, several steps have to be performed before a secure ATM connection in the wireless ATM communication network can be guaranteed. This will be explained below with reference to Fig. 1b and Fig. 2.

Conventional authentication procedure

[0010] Fig. 1b shows a simplified network configuration according to Fig. 1a for explanation purposes. Fig. 1b represents a typical case when the wireless ATM system is a wireless LAN or a broadband access system, where it is desirable that a wireless ATM radio communication network WATM is to be connected to a fixed non-ATM system, for example to an Ethernet via access nodes AN of the WATM system and the FN system. Typically, the Ethernet only supports one secure association establishment protocol.

[0011] However, in Fig. 1b the Ethernet is only taken as an example for the non-ATM fixed network and it may be useful to connect a general wireless ATM radio communication network WATM to a network system through access nodes AN, wherein the network system can perform different secure association establishment procedures. Of course, this implies that a signaling gateway is established between the network system and the WATM system.

[0012] As is also shown in Fig. 1b, a wireless communication connection WCC is set-up between the ATM mobile terminal MT and the ATM access node AN and the ATM signaling is thus terminated in the access node AN. It is generally difficult to design services within the WATM system if these services should rely on functions and services in the fixed networks exactly because the ATM signaling is terminated in the access point AN.

[0013] With the access node AN clearly being the entry point into the WATM system, it is obvious that the access node AN has to be protected against fraudulent and accidental misuse, such that not any subscriber can have access to the WATM system. As explained before, this is done by a two step mechanism, namely an authentication mechanism where the mobile station MT and the access node AM must recognize each other, and a second step where encryption methods are used on the radio link to provide a confidentiality level on the radio link. Thus, not any arbitrary subscriber station SS, for example from the fixed network SN, should gain an access and should be supported in the WATM system, but only such subscriber stations for mobile stations which are recognized by the WATM system.

[0014] When a mobile terminal MT desires an access to the WATM system or requires a registration, the following two types of registrations can be distinguished:

1. The access node AN and the ATM mobile terminal MT must possess a secret authentication information AI and the authentication information must be the same in the access node AN and in the mobile terminal MT. Such an authentication information may typically be an authentication key or a challenge/response information.

2. The ATM mobile terminal MT and the access node AN "don't know each other"; i.e. they cannot recognize each other.

[0015] In both cases, communication keys (encryption/decryption keys) have to be generated and exchanged between the mobile terminal MT and the access node AN in any case. These communication keys CK are used to achieve a confidentially of the information transmitted on the wireless ATM connection. Protocols which are used to generate and exchange such communication keys CK are generally called "key agreement protocols" and in existing networks like GSM, DECT, IS-54, IS 95 and CDPD, they are combined with the subscriber authentication, thus building a so-called "atomic authentication and key agreement (AKA) protocol".

[0016] Generally, there are two categories of AKA protocols that can be used for setting up the communication between the ATM mobile terminal MT and the ATM access node AN. Namely, the first category comprises for example the usage of the Diffie-Hellman encrypted key exchange (DH-EKE) protocol or the simple key exponential key exchange (SPEKE) protocol (see e.g. reference [1]: B. Schneier, "Applied Cryptography, Second Edition, Wiley, 1992" and reference [2]: D. Jablon "Strong Passwork only Authenticated Key Exchange, ACM Computer Communication Review, October 1996"). A typical flow chart of how a secured communication between ATM mobile terminal MT and an ATM access node AN of a wireless ATM radio communication network WATM using this kind of protocol is achieved, is illustrated in Fig. 2.

[0017] In Fig. 2, the mobile terminal MT and the access node AN exchange authentication information in step ST2 after starting the setup procedure in step ST1. In ST3 it is checked whether the mobile terminal MT and

the access point AP recognize each other, i.e. whether the access node AN have stored an authentication information which coincides with that sent by the mobile terminal MT. It this is not so, "N" in step ST3, the exchange of authentication information is repeated in step ST2. If the mobile terminal MT and the access point AM use the same authentication information, "Y" in step ST3, then the MT and the access node AN agree on a secrete ciphering key in step ST4 (using the AKA protocol). If MT/AN have agreed on a secret session key (communication or ciphering key) in step ST4, then a secure wireless ATM communication connection WCC has been established and the usual communication signaling protocol for information transfer can be setup in step ST5. The setup procedure comes to an end in step ST6.

[0018] Therefore, using the conventional Diffie or Diffie-Hellman encrypted key exchange (DH-EKE) or the simple key exponential key exchange (SPEKE) protocol, the authentication information AI is in fact established before completing the AKA protocol. However, there is a second category of AKA protocols, where the secret shared authentication information is not available before setting up the wireless communication connection WCC based on the agreed session encryption keys. That is, using protocols of the second category means that the shared authentication information only becomes available after, the secured communication connection has been set up.

[0019] As is illustrated in Fig. 1b, the situation becomes even more difficult if different signaling protocols are used on the wireless ATM communication connection WCC between the mobile terminal MT and the access node AN (i.e. an WATM signaling) and between the access node AN of the WATM network and the access nodes AN of the fixed networks SN, for example an internet signaling or an UMTS signaling. That is, if the access of the AN of the WATM communication network should be flexible enough to interconnect to different signaling protocols (for example internet signaling or UMTS signaling) then different authentication procedures or different AKA protocols may have to be used dependent on the used protocol between the ATM system and the fixed network FN. Therefore, sometimes the category 1 AKA protocol may have to be used and some times the category 2 AKA protocol may have to be used. Thus, in some cases the authentication information may not be available before setting up the encrypted ATM wireless communication connection WCC.

Summary of the Invention

[0020] As described above, the problem with setting up ATM wireless communication connections between a ATM mobile terminal and a ATM access node essentially resides in the fact, that either different kinds of AKA protocols are to be set up to the access node or that in fact the authentication information is not available prior to completing the AKA protocol.

[0021] Therefore, the object of the present invention is to provide a method, an authentication device, an ATM access node, an ATM mobile terminal as well as a ATM communication system, in which a secure communication between a ATM mobile terminal and an ATM access node can be established.

[0022] A secure communication is preferably to be established even if the authentication information is not available when completing the protocol or if various different AKA protocols are to be used on the access node or if security mechanisms of other interconnected networks are to be used.

Solution of the Object

[0023] Essentially this object is solved by a method for setting up a secured communication between an ATM mobile terminal and an ATM access node of a wireless ATM radio communication network, comprising the step of setting up a wireless ATM radio communication connection between said ATM mobile terminal and said ATM access node without performing an authentication information checking procedure therebefore, wherein an information exchange on said wireless ATM radio communication connnection is performed by using a secret communication key agreed upon by said ATM access node and said ATM mobile terminal.

[0024] Furthermore, this object is solved by an authentication device, in particular for a wireless ATM radio communication network, comprising, an authentication information storage means for storing a plurality of authentication informations each corresponding to a respective ATM mobile terminal served by a wireless ATM radio communication network, and an authentication information transmisssion means for issuing an authentication information in reponse to receiving an authentication information request from an ATM mobile terminal after a ATM wireless radio communication connection has been setup between said requesting ATM mobile terminal and said ATM access node using a secret communication key agreed upon by said ATM access node and said ATM mobile terminal.

[0025] The object is also solved by an ATM access node of a wireless ATM communication network for setting up a secured wireless ATM communication connection to an ATM mobile terminal, said ATM access node comprising, a setup means for setting up a wireless ATM radio communication connection to said ATM mobile terminal without performing an authentication information checking procedure therebefore, a secret communication key storage means for storing a secret communication key used by said ATM mobile terminal and said ATM access node for performing wireless ATM communications.

[0026] Furthermore, the object is solved by an ATM mobile terminal for setting up a secured communication

ISDOCID: <EP___0939571A1_I_>

to an ATM access node of a wireless ATM communication network, comprising, a setup means for setting up a wireless ATM radio communication connection to said ATM access node without performing an authentication information checking procedure therebefore, a secret communication key storage means for storing a secret communication key used by said ATM mobile terminal and said ATM access node for performing wireless ATM communications.

[0027] Finally, the object is also solved by an ATM wireless communication network according to claim 32.

[0028] The basic idea of the invention is to provide user chosen confidentiality level on the radio link by means of setting up a secure association between the WATM access node and the wireless ATM mobile terminal without using an authentication as a first step. That is, according to the invention, a wireless ATM radio communication connection is established by agreeing upon a secret communication key CK between the ATM access node and the ATM mobile terminal, wherein no authentication information checking procedure is performed therebefore.

[0029] Another aspect of the invention is that once the secured wireless ATM radio communication connection has been established between the mobile terminal and the access node, the mobile terminal tries to get the secret shared authentication information by use of higher level protocols communication from an authentication device provided in the wireless ATM communication network or provided in a network which is connected to the access node (with which the mobile terminal has setup the secure ciphered communication link) through a signalling path. This authentication device comprises an authentication information search means for storing a plurality of authentication informations each corresponding to a respective ATM mobile terminal served by said wireless ATM radio communication network. When the ATM communication connection has been set up, the mobile terminal requests an authentication information from this authentication device and only then an authentication procedure is performed at the access node with the authentication information being provided by the authentication device.

[0030] Another aspect of the invention is that the mobile terminal must receive the secret shared authentication information from the authentication device within a predefined period or within a period which has been negotiated between the mobile terminal and the access node. If the mobile terminal receives the secret shared authentication information within this period, then it either authenticates itself at the access node or this task is being taken care of by the authentication device which initially provided the authentication information.

[0031] If the time runs out, i.e. if the mobile terminal cannot authenticate itself at the access node within the predefined time period, then the already setup wireless ATM radio communication connection is interrupted (closed) and information regarding the mobile terminal (which has unsuccessfully attempted an authentication) is stored in the access node. Preferably, if the same mobile terminal has already failed an authentication a predetermined number of times, then further access requests from this mobile terminal are immediately rejected by the access node.

[0032] Preferably, before the authentication procedure is performed at the access node, the mobile terminal (the user) can choose a predetermined communication key (confidentiality level) to be used on the wireless ATM communication connection. Thus, the user or the user application itself can choose the degree of confidentiality which it desires on the wireless communication connection.

[0033] If the authentication device is located or part of the WATM system a signalling path is established through the access node to the authentication device in order to request the authentication information. This information is then preferably transferred back to the mobile terminal through the already setup ciphered communication link.

[0034] If the authentication device is located or part of another network connected to the access node via a communication link, depending on the type of WATM network and the type of the connected network, a signalling path is setup to the authentication device through the access node to request the authentication information. Preferably, this authentication information is again transferred back to the mobile terminal along the already setup communication (ciphered) channel.

[0035] Further advantageous embodiments and improvements of the invention may be taken from the dependent claims. Hereinafter, the invention will be described with reference to its advantageous embodiments and the attached drawings.

Brief Description of the Drawings

[0036] In the drawings:

Fig. 1a shows a principle overview of possible network configurations including a wireless ATM network;

Fig. 1b shows an example where a wireless ATM system WATM is connected to a fixed network FN through access nodes AN;

Fig. 2 shows a conventional method to setup a secured communication between ATM mobile terminal and an ATM access node;

Fig. 3 shows an authentication device SSD, an access node AN and a mobile terminal MT according to the invention;

Fig. 4 shows a principle flowchart of the method

according to the invention;

Fig. 5 shows a more detailed flowchart of setting up a secured communication according to the invention.

Principle of the Invention

[0037] As explained before, one of the big disadvantages of the existing secret-based AKA protocols is that the shared authentication information has to be established between the mobile terminal MT and the access node AN prior to completing the protocol. However, when different signaling protocols are used on the wireless link between the mobile terminal MT and the access node AN (WATM signaling) and between the access node AN and other fixed network nodes, (e.g. internet signaling) then the setup of shared secret knowledge prior to secure association might be extremely difficult. This happens also when the access node AN is not connected to a fixed ATN network. In such case, some protocols might be used (e.g. Diffie-Hellman) to build out a temporary security association between AN and NT, i.e. to setup shared secret keys for radio link encryption. After setting a secure channel a regular end-to-end authentication might be done.

[0038] According to the invention a method is established that provides a user chosen confidentiality level on the radio link by means of setting up a secure association between the WATM access point and the wireless ATM terminal without any authentication in the first run. After the secure association has been established, for example using an unauthenticated variant of the conventional protocol, the mobile terminal MT tries to get the secret shared authentication information by communicating with an authentication device (also called a security server) in the WATM network (or in fact in an interconnected fixed network) through a communication (signalling) channel setup means of a higher level protocol. The transfer of the authentication information then takes place along the already setup ciphered communication channel.

[0039] If the mobile terminal gets to secret shared authentication information within a predefined or negotiated period, it performs an authentication itself at the access node AN. This authentication procedure can be accomplished using either an authenticated variant of the flexible AKA protocol or other mechanisms. Otherwise, the respective timer in the access node AN runs out and the access AN closes to wireless connected to the mobile terminal MT. Attacks of fraudulent or accidental misuse can be prevented to some extent by storing the MAC address or other suitable information about the mobile terminal MT within the access point AN. After N unsuccessful connection setups further access requests from this mobile terminal MT are immediately rejected by the access node AN.

[0040] Therefore, whilst all AKA protocols in the prior art use an authentication procedure before setting up the actual wireless ATM communication connection, one of the basic principles of the invention is based on the idea to first setup the wireless ATM communication between the mobile terminal MT and the access node AN by selecting and agreeing upon a common encryption communication key and only thereafter possibly an authentication is performed.

[0041] Embodiments of the mobile terminal MT, access node AN and the authentication device of the WATM system performing such a function are described below with reference to Fig. 3. It should be understood that Fig. 3 in principle corresponds to Fig. 1b, i.e. a plurality of mobile terminals MT are connected to a wireless ATM system and a wireless secured ATM communication connection WCC is to be set up between the mobile terminals MT and the access node AN.

Embodiment of the mobile terminal MT/Access node AN

[0042] Hereinafter, the functions performed by the mobile terminal MT and the access node AN according to the invention as shown in Fig. 3 will be illustrated with reference to the communication connection setup method as shown in Fig. 4.

[0043] In Fig. 3 the ATM mobile terminal MT comprises a setup means MT-SET for setting up a wireless ATM radio communication connection WCC to said ATM access node AN. Likewise, the access AN comprises a setup means AN-SET for setting up the wireless ATM radio communication connection WCC to said ATM mobile terminal MT. In the mobile terminal MT and the access node AN a respective secret communication key KC storage means CK-MEM stores a secret communication key CK used by said ATM mobile terminal MT and said ATM access node AL for performing wireless ATM communications. After starting the setup procedure in step S1 in Fig. 4, the setup means MT-SET of the mobile terminal MT sends a setup request to the access node AN by means of a protocol, to setup a secure association, i.e. a secured wireless ATM radio communication connection WCC to said setup means AN-SET of the access node AN. As is seen in Fig. 4, there is no authentication procedure before or after the setting up procedure in S2. That is, in step S2 a fully operable (i.e. usable for data transfer) and ciphered wireless ATM radio communication link is setup which uses a secret communication key CK, (i.e. a confidentiality level or encryption key) which has been agreed upon by said ATM mobile terminal MT and said ATM access node AN for performing wireless ATM communications.

[0044] In step S2, a secrete key selection means MT-SEL of said mobile terminal MT can preferably predefine or select one of a plurality of secret communication keys CK stored in the secret communication key storage

means CK-MEM within the mobile terminal MT. That is, in step S2, the user or the user application can predefine a desired confidentiality level on the wireless ATM radio communication connection WCC.

[0045] First, in step S2 a user chosen confidentiality level can preferably be provided on the radio link by means of setting up a secure association between the WATM access node AN and the wireless ATM mobile terminal without an authentication in the first run. Thus, by contrast to the category 1 AKA protocols, the protocol illustrated in fig. 4 does not require the setup of shared authentication information between the mobile terminal MT and the access node AN prior to completion of the protocol. The procedure is also applicable to category 2 protocols, because there is yet again no necessity to setup the secret shared authentication information before setting up the security association (i.e. the encryption key). Thus, the procedure in Fig. 4 is intrinsically different to what was described above for the category 1, category 2 setup protocols, since an authentication information agreement is not necessary before setting up of the operable wireless ATM radio communication connection WCC.

[0046] After step S2 immediately the real communication protocol for information transfer between MT/AN can be set up in step S6 whereafter the setup procedure comes to an end in step S7.

Inclusion of the Authentication Information

[0047] Whilst there is no necessity to perform an authentication before the setup of the communication channel WCC in Fig. 3, 4, preferably such an authentication procedure may be carried out after step S2, as is shown in more detail in the flow chart in Fig. 5.

[0048] To realize this authentication procedure, the wireless ATM network WATM (or any interconnected non-ATM or ATM fixed network) preferably comprises an authentication device SSD comprising an authentication information storage AI-MEM for storing a plurality of authentication informations AI each corresponding to a respective ATM mobile terminal MT served by said wireless ATM radio communication network WATM. Furthermore, the device SSD comprises an authentication information transmission means TR for issuing an authentication information AI in response to receiving an authentication information request AI-RQST from an ATM mobile terminal MT after said ATM wireless radio communication connection WCC has been setup between the ATM mobile terminal MT and said ATM access node AN.

[0049] Instead of just exchanging authentication information between MT and AN, an authentication means MT-AN of the mobile terminal MT requests an authentication information from the authentication device SSD (hereinafter also called a security server) of the WATM network (or the interconnected fixed network FN) through higher layer protocols in step S3. This request message is denoted AI-RQST in Fig. 3. In response to said request message AI-RQST, the security server SSD reads out from the memory AI-MEM an authentication information corresponding to the mobile terminal MT requesting such information. It the requesting mobile terminal MT is an admitted (subscribed) mobile terminal MT, then the security server SSD should have an entry for this mobile terminal MT in the memory AI-MEM.

[0050] In response to such a request AI-RQST the mobile terminal MT is authenticated at the access node AN. This can take place either by the security server SSD transferring the requested authentication information AI directly to the access node AN or alternatively the security server SSD returns the authentication information AI to the mobile terminal MT via the already established secured (ciphered) communication channel WCC. At the mobile terminal the authentication information AI is received in an authentication information reception means MT-RM.

[0051] Having established the secured communication connection WCC between the mobile terminal MT and the access node AN authentication information AI provided by an authentication device SSD located within the WATM system or even an interconnected network can now be transferred back to the mobile terminal MT in a secured or ciphered manner through the communication connection WCC.

[0052] Then the mobile terminal MT itself performs the authentication procedure with the access node AN by transferring the received authentication information AI to the access node AN. In both scenarios, the ATM mobile terminal MT is authenticated at the ATM access node by means of the transfer of the authentication information AI which identifies the ATM mobile terminal MT at the ATM access node AN. Therefore, if an authentication information reception means AI-RM in the access node AN receives an authentication information AI, an authentication means AN-RN in said ATM access node AN performs the authentication of the ATM mobile terminal MT when the received authentication information AI is one that identifies the requesting ATM mobile terminal MT as an admitted ATM mobile terminal MT.

[0053] Therefore, no matter where to the authentication information transmission means AI-TR of the security server SSD transmits the authentication information AI, an authentication procedure can always be performed successfully in step S5 if the authentication information AI is one that is recognized by said access node AN. That is, an authentication means MT-AN of said ATM mobile terminal can send an authentication information request message AI-RQST in step S3 in Fig. 5 to the network authentication device SSD and an authentication information reception means MT-RM receives that authentication information AI from said network authentication device SSD in response to the request message. Alternatively, the access node

authentication means AN-AM performs the authentication on the basis of authentication information received from the security server directly.

[0054] Preferably, after the access node AN has finalized the setup of the wireless communication connection WCC to said mobile terminal MT, a timer TMR in said access node AN can be set in step S2 in Fig. 5. Preferably, the timer TMR in AN sets a predetermined time period in which an authentication information reception by AI-RM in AN is expected. Therefore, independently as to whether the authentication information AI is transmitted by the security server SSD or the mobile terminal MT itself, in step S4 a determination is made by the timer TMR in AN as to whether or not the authentic information AI has been received in a predetermined time period. If it has been received, "Y" in step S4 in Fig. 5, then the normal authentication procedure can be performed in step S5. If "N" in step S4, then the timer TMR in AN waiting for the input of the authentication information from MT (directly or through SSD) runs out. In this case, the previously setup wireless ATM communication connection WCC is closed in step S8 by an interrupt means INT in AN .

[0055] Preferably, an identity memory ID-MEM stores an identity information II, MAC of the ATM mobile terminal MT whose communication connection WCC has been released (closed). The identity information can for example be the MAC address of the requesting mobile terminal MT (MAC: Mobile Access Code).

[0056] Furthermore, if the access node AN recognizes that the mobile terminal MT presently requesting an authentication has already previously been trying to setup a communication to the access node AN, also the number of retries MTr can be compared with a maximum number of retries N in step S10. If the same mobile terminal MT has requested an authentication more than N times, then an access node inhibition means AN-INBT will completely inhibit or reject any further setup requests from this mobile terminal MT in step S11, whereafter the procedure comes to an end in step S12.

[0057] The interrupt means INT in the ATM access node AN is responsible for closing an already set up secure wireless radio communication WCC, if said authentication information reception means AI-RM does nor receive the authentication information from MT within the predetermined time period as is determined by the timer TRM in AN. If "N" in step S10, the procedure goes back to step S2 to allow the setup of a communication connection WCC again in step S2.

[0058] Preferably, also the ATM mobile terminal MT comprises a timer TMR and if after said sending of said authentication information request message AI-RQST an authentication information AI is not received from said network authentication device or security server SSD within a predetermined period, an interrupt means MT-IM of said ATM mobile terminal MT will close the setup wireless ATM radio communication networks WCC itself. The reason is, that at this point it can hardly be expected that the security service SSD of the WATM system will return an authentication information AI, i.e. that it is hardly likely that the mobile terminal MT has really a valid subscription for setting up communication connections in the WATM communication system.

[0059] Preferably, the ATM mobile terminal MT also comprises an automatic repetition means MT AUTO for automatically repeating a setup attempt after a predetermined time interval. That is, even before the security server SSD returns a negative response, i.e. that no authentication information can be found in the memory AI-MEM for the presently calling mobile calling MT, the mobile terminal MT can automatically again request the setup of a communication connection WCC to said access node AN.

[0060] If the mobile terminal MT has performed a predetermined number of repetitive setup requests, as counted by a counter MT-CNT, then an inhibition means MT-INHB of the mobile terminal MT inhibits any further setup requests after a predetermined number N of attempts.

[0061] Therefore, not only the access node AN can reject further setup requests by the same mobile terminal MT but also the mobile terminal MT itself may decide and recognize that in fact the security server SSD has no information stored whatsoever that would indicate that the presently calling mobile terminal MT is one that has been registered for wireless ATM connections to said access node AN.

[0062] Therefore, the above novel protocol can be summarized as follows (see also Fig. 5):

S2: Setup a secure association (a secured communication connection WCC) between the mobile terminal MT and the access node AN without any authentication procedure; start a timer TMR in the access node;

S3/S4: If the mobile terminal MT gets secret shared authentication within the predetermined time period through the ciphered communication channel WCC then the authentication takes place. If not, the access node interrupt means INT interrupts or closes the already setup communication connection WCC in step S8.

S5: Either the mobile terminal MT authenticates itself at the access node AN or the security server authentication device SSD authenticates the mobile terminal at the access node AN. If there is no time out by the timer TMR in the access node AN or the timer TMR in the mobile terminal MT, the general communication protocol for information transfer is set up between MT and AN in step S6.

Industrial Applicability

[0063] As explained above a secure setup of a communication connection between MT and AN is established even if no authentication can be performed in the first run as explained with reference to Fig. 4. Authentication is performed afterwards either between MT and AN or between the authentication device SSD and AN. This is useful for example in a wireless ATM mobile terminal without hardware support for storing authentication information (e.g. a SIM card).

[0064] By the provision of the communication key memory CK-MEM, the operator of the mobile terminal MT or in fact the user application itself can establish a user-chosen confidentiality level without following authentication, e.g. to allow access of mobile terminals MT to networks in semi-public areas (e.g. airports). First, for example a user-application like a program running on a LAPTOP can - without a hardware support for storing authentication information like a SIM card - request an authentication information from a security server SSD and if a registration of such an authentication information has been previously performed in the memory AI-MEM of the security server SSD, than an access of the mobile terminal MT to the network is granted.

[0065] Furthermore, it should be noted that the authentication device SSD does not necessarily have to be a part of the WATM system. It can also be a part of the interconnected ATM fixed network which is shown in Fig. 2. However, confidentiality of user data on the ATM wireless radio connection WCC can be guaranteed, even if the fixed network is only involved after the setup of the security association, for example if the authentication information is requested from a security server SSD of the fixed network and is then - in a secure ciphered manner - transferred back to the mobile terminal through the secured communication channel.

[0066] Thus, a security service SSD for WATM systems can be implemented, that can be used in a non-ATM fixed network environment, i.e. if ATM calls are only used on the wireless radio link in the WATM system, whilst an ordinary digital transmission is used in the fixed network. Again, since the confidentiality is ensured on the wireless communication connection WCC, the authentication information can be requested and supplied by any security server SSD which is located even in the fixed network environment. This means that the transfer of the authentication information takes place along a wireless ATM communication connection which is already secured by the agreed selected secret ciphering key CR.

[0067] However, the inventive method, authentication device, mobile terminal and the access node can also be used in cases, where an ATM based fixed network implements security services on top of the ATM layer. This means, if the fixed network system is also an ATM-based fixed network, first the communication channel WCC with its confidentiality level is setup between the mobile terminal MT and the access node AN of the wireless ATM system (or in fact to an access node AN of the ATM-based fixed network) and thereafter the (secured) authentication information exchange is performed. For requesting and receiving the authentication information from a security server SSD of the ATM-based fixed network, a separate signaling channel from the access node AN of the WATM system to the access node AN of the ATM-based fixed network is preferably used.

[0068] The present invention provides confidentiality in different wireless ATM systems which are adapted for private and/or business and/or public environments or even mixed environments. Since the communication channel WCC is setup before a possible authentication procedure, there is provided the major advantage that security mechanisms within the WATM system or even security mechanisms from possibly interconnected fixed networks (non-ATM or ATM) can be accessed through the secured link WCC or can even be combined, in order to build a security architecture that offers much higher security level. Since the mobile terminal MT has access to the security functions located elsewhere in an interconnected network, a security architecture can be built, which is more flexible and which can offer a much higher security level.

[0069] Whilst the invention has been described with reference to its embodiments and the drawings to illustrate what is currently considered as the best mode of the invention, it is clear, that various modifications and variations will be possible for those skilled in the art in view of the above technical teachings. Therefore, the invention is not restricted to the present description and the scope of the invention is defined by the attached claims. In these claims, reference numerals only serve clarification purposes and to not limit the scope of the invention. In the drawings the same or similar reference numerals designate the same or similar parts or steps.

Claims

1. A method for setting up a secured communication between an ATM mobile terminal (MT) and an ATM access node (AN) of a wireless ATM radio communication network (WATM), comprising the step of setting up (S2) a wireless ATM radio communication connection (WCC) between said ATM mobile terminal (MT) and said ATM access node (AN) without performing (ST2, ST3) an authentication information checking procedure therebefore, wherein an information exchange on said wireless ATM radio communication connnection (WCC) is performed by using a secret communication key (CK) agreed upon by said ATM access node (AN) and said ATM mobile terminal (MT).

2. A method according to claim 1, *characterized in that*

after said setting up of said wireless ATM radio communication connection (WCC) between said ATM mobile terminal (MT) and said ATM access node (AN) is completed (S2), said ATM mobile terminal (MT) is authenticated (S3, S5; S4, S8) at said ATM access node (AN) by transferring authentication information (AI) identifying said ATM mobile terminal (MT) to said ATM access node (AN).

3. A method according to claim 2, *characterized in that* said ATM mobile terminal (MT) sends an authentication information request message (AI-RQST, S3) to a network authentication device (SSD) provided by said wireles ATM communication network (WATM) or by a further interconnected network (FN).

4. A method according to claim 3, *characterized in that* said authentication information (AI) is transferred (S4) to said ATM mobile terminal (MT) in response to said request message (AI-RQST) and said ATM mobile terminal (MT) performs an authentication procedure at said ATM access node (AN) using said transferred authentication information (AI).

5. A method according to claim 3, *characterized in that* in response to said request meassage (AI-RQST), said network authentication device (SSD) of said wireless ATM communication network (WATM) performs (S5) an authentication procedure for said ATM mobile terminal (MT) at said ATM access node (AN) using said requested authentication information (AI).

6. A method according to claim 2, *characterized in that* after said secure wireless ATM radio commmunication connection (WCC) has been set up (S2), a timer (TMR) in said ATM access node (AN) is started and said already setup wireless ATM radio commmunication connection (WCC) is closed by said ATM access node (AN) if said ATM access node (AN) does not receive an authentication information (AI) for said ATM mobile terminal (MT) within a predetermined time period (S8).

7. A method according to claim 6, *characterized in that* identity information (II, MAC)) of said ATM mobile terminal (MT) and the number of authentication retries (MTr) is stored (ID-MEM) in said ATM access node (AN) if said ATM access node (AN) does not receive said authentication information (AI) within said predetermined time period (S9).

8. A method according to claim 7, *characterized in that* when said number of authentication retries (MTr) exceeds (S10) a predetermined number (N), further requests by said ATM mobile terminal (MT) to set up a wireless ATM radio communication connection (WCC) between said ATM mobile terminal (MT) and said ATM access node (AN) are rejected (S11) by said ATM access node (AN).

9. A method according to claim 1, *characterized in that* said secret communication key (CK) is selected by said ATM mobile terminal (MT) during the setting up of the wireless ATM radio communication connection (WCC).

10. A method according to claim 1, *characterized in that* to said wireless ATM radio communication network (WATM) access node (AN) is connected a non-ATM fixed network (FN) providing functions and services to a plurality of fixed network subscribers (SS), wherein said ATM mobile terminal (MT) accesses said functions and services via said secured wireless ATM radio communication connection setup between said ATM mobile terminal (MT) and said ATM access node (AN).

11. An authentication device (SSD), in particular for a wireless ATM radio communication network (WATM), comprising:

a) an authentication information storage means (AI-MEM) for storing a plurality of authentication informations (AI) each corresponding to a respective ATM mobile terminal (MT) served by a wireless ATM radio communication network (WATM); and

b) an authentication information transmisssion means (TR) for issuing an authentication information (AI) in reponse to receiving an authentication information request (AI-RQST) from an ATM mobile terminal (MT) after a ATM wireless radio communication connection (WCC) has been setup between said requesting ATM mobile terminal (MT) and said ATM access node (AN) using a secret communication key (CK) agreed upon by said ATM access node (AN) and said ATM mobile terminal (MT).

12. A device according to claim 11, *characterized in that* said transmission means (AI-TR) is adapted to transfer said authentication information (AI) back to said requesting ATM mobile terminal (MT).

13. A device according to claim 11,
characterized in that
said transmission means (AI-TR) is adapted to transfer said authentication information (AI) to said ATM access node (AN) to perform an authentication procedure for said ATM mobile terminal at said ATM access node (AN).

14. A device according to claim 11,
characterized in that
to said wireless ATM radio communication network (WATM) access node (AN) is connected a non-ATM fixed network (FN) providing functions and services to a plurality of fixed network subscribers (SS), wherein said ATM mobile terminal (MT) access said functions and services via said secured wireless ATM radio communication link setup between said ATM mobile terminal and said ATM access node (AN).

15. An ATM access node (AN) of a wireless ATM communication network (WATM) for setting up a secured wireless ATM communication connection (WCC) to an ATM mobile terminal (MT), said ATM access node (AN) comprising:

a) a setup means (AN-SET) for setting up (S2) a wireless ATM radio communication connection (WCC) to said ATM mobile terminal (MT) without performing (ST2, ST3) an authentication information checking procedure therebefore;

b) a secret communication key (CK) storage means (CK-MEM) for storing a secret communication key (CK) used by said ATM mobile terminal (MT) and said ATM access node (AN) for performing wireless ATM communications.

16. An ATM access node (AN) according to claim 15,
characterized by
an authentication means (AN-AM) for authenticating said ATM mobile terminal (MT) at said access node (AN) when an authentication information reception means (AI-RM) receives authenticaton information (AI) identifying said ATM mobile terminal (MT).

17. An ATM access node (AN) according to claim 16,
characterized in that
said authentication information reception means (AI-RM) receives said authentication information (AI) from said ATM mobile terminal (MT).

18. An ATM access node (AN) according to claim 16,
characterized in that
said authentication information reception means (AI-RM) receives said authentication information (AI) from a network authentification device (SSD) separately provided by said wireless ATM radio communication network (WATM) or by a further or interconnected network (FN).

19. An ATM access node (AN) according to claim 16,
characterized in that
said ATM access node (AN) comprises a timer (TMR), which is started after said wireless ATM communication connection (WCC) between said access node (AN) and said ATM mobile terminal (MT) has been setup by said setup means (AN-SET).

20. An ATM access node (AN) according to claim 19,
characterized in that
said ATM access node (AN) comprises an interrupt means (INT) for closing an already setup secured wireless radio commmunication connection (WCC) if said authentication information reception means (AI-RM) does not receive an authentication information for said ATM mobile terminal (MT) within a predetermined time period (S8) as determined by said timer (TMR).

21. An ATM access node (AN) according to claim 20,
characterized in that
identity information (II, MAC)) of said ATM mobile terminal (MT) and the number of authentication retires (MTr) is stored in an identity memory (ID-MEM) in said ATM access node (AN) if said authentication information reception means (AI-RM) does not receive said authentication information (AI) within said predetermined time period (S9).

22. An ATM access node (AN) according to claim 21,
characterized in that
when said number of authentication retries (MTr) exceeds (S10) a predetermined number (N), an inhibiting means (AN-INBT) of said ATM access node (AN) inhibits further requests by said ATM mobile terminal (MT) to set up a wireless ATM radio communication connection (WCC) between said ATM mobile terminal (MT) and said ATM access node (AN).

23. An ATM access node (AN) according to claim 15,
characterized in that
to said ATM access node (AN) is connected a non-ATM fixed network (FN) providing functions and services to a plurality of fixed network subscribers (SS), wherein said ATM mobile terminal (MT) accesses said functions and services via said wireless ATM radio communication link setup between said ATM mobile terminal and said ATM access node (AN).

24. An ATM mobile terminal (MT) for setting up a

secured communication (WCC) to an ATM access node (AN) of a wireless ATM communication network (WATM), comprising:

a) a setup means (MT-SET) for setting up (S2) a wireless ATM radio communication connection (WCC) to said ATM access node (AN) without performing (ST2, ST3) an authentication information checking procedure therebefore;

b) a secret communication key storage means (CK-MEM) for storing a secret communication key (CK) used by said ATM mobile terminal (MT) and said ATM access node (AN) for performing wireless ATM communications.

25. An ATM mobile terminal (MT) according to claim 24,
characterized in that
an authentication means (MT-AM) of said ATM mobile terminal (MT) sends an authentication information request message (AI-RQST; S3) to a network authentication device (SSD) provided by said wireles ATM communication network (WATM) or an interconnected fixed network (FN).

26. An ATM mobile terminal (MT) according to claim 25,
characterized in that
an authentication information recepetion means (MT-RM) receives said authentication information (AI) from said network authentication device (SSD) in response to said request message (AI-RQST).

27. An ATM mobile terminal (MT) according to claim 26,
characterized in that
said authentication means (MT-AM) transfers said received authentication information (AI) to said ATM access node (AN).

28. An ATM mobile terminal (MT) according to claim 25 and 26, *characterized in that*
said ATM mobile terminal (MT) comprises a timer (TMR) and if after said sending of said authentication information request message (AI-RQST) an authentication information (AI) is not received from said network authentication device (SSD), an interrupt means (MT-IM) of said ATM mobile terminal (MT) closes said setup wireless ATM radio communication connection (WCC) between said mobile terminal (MT) and said ATM access node (AN)

29. An ATM mobile terminal (MT) according to claim 25,
characterized in that
said ATM mobile terminal (MT) comprises an automatic repetition means (MT-AUTO) for automatically repeating a setup attempt after a predetermined time intervall.

30. An ATM mobile terminal (MT) according to claim 29,
characterized in that
said ATM mobile terminal (MT) comprises a counter (MT-CNT) which counts the number of repetitive attempts to setup a connection by said setup means (MT-SET), wherein an inhibition means (MT-INHB) inhibits further setup requests after a predetermined number (N) of attempts.

31. An ATM mobile terminal (MT) according to claim 24,
characterized by
a secret key selection means (MT-SEL) for selecting a secret key (CK) used for the wireless ATM communication connection (WCC).

32. An ATM wireless communication network (WATM), comprising at least one ATM mobile terminal (MT) according to one or more of claims 24-31, at least one ATM access node (AN) according to one or more of claims 15-23 and an exchange means (EX) for setting up ATM wireless radio communcication connections (WCC) between said at least one mobile terminal (MT) and said at least one ATM access node (AN).

33. An ATM wireless communication network (WATM) according to claim 32, *characterized in that*
to said wireless ATM radio communication network (WATM) is connected a non-ATM fixed network (FN) providing functions and services to a plurality of fixed network subscribers (SS), wherein said ATM mobile terminal (MT) accesses said functions and services via said wireless ATM radio communication connection (WCC) setup between said ATM mobile terminal (MT) and said ATM access node (AN).

34. A method according to claim 4,
characterized in that said authentication information (AI) is transferred back to said mobile terminal (MT) through said setup secured communication connection (WCC).

35. A device according to claim 12,
characterized in that said transmission means (TR) transfers back said authentication information to said mobile terminal (MT) through said setup secured communication connection (WCC).

36. An access node (AN) according to claim 16,
characterized in that a transmission means (TR) of said access node (AN) transfers back said authentication information to said mobile terminal (MT)

EPODOC: <EP___0939571A1 I >

through said setup secured communication connection (WCC).

37. An ATM mobile terminal (MT) according to claim 26,
characterized in that said authentication information reception means (MT-RM) receives said authentication information (AI) through said setup secured communication connection (WCC) setup between said access node (AN) and said ATM mobile terminal (MT).

38. An ATM mobile terminal (MT) according to claim 27 characterized in that said authentication means (MT-AM) transfers said authentication information (AI) through said secured communication connection (WCC) setup between said access node (AN) and said ATM mobile terminal (MT) to said access node (AN).

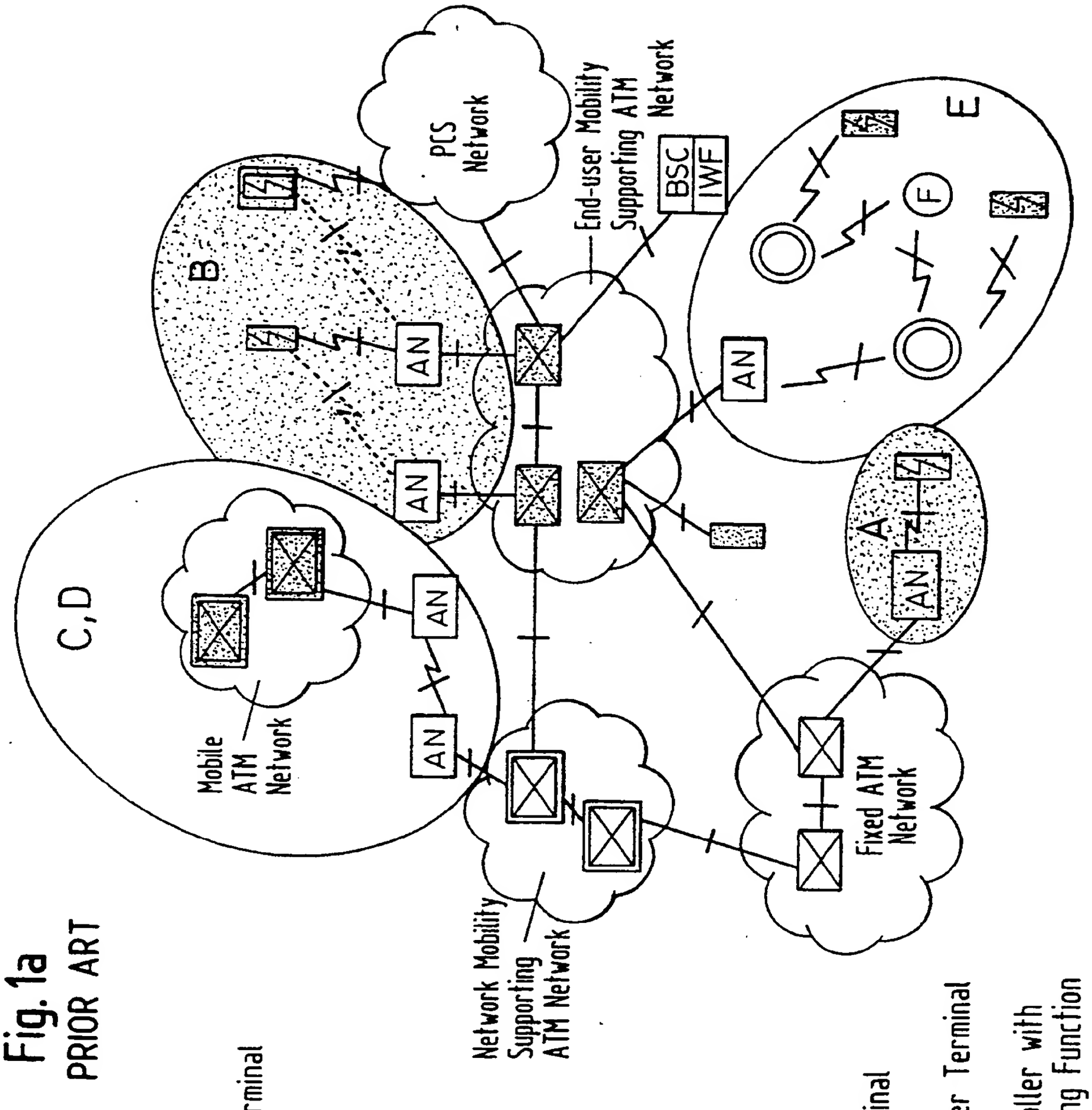


Fig. 1a
PRIOR ART

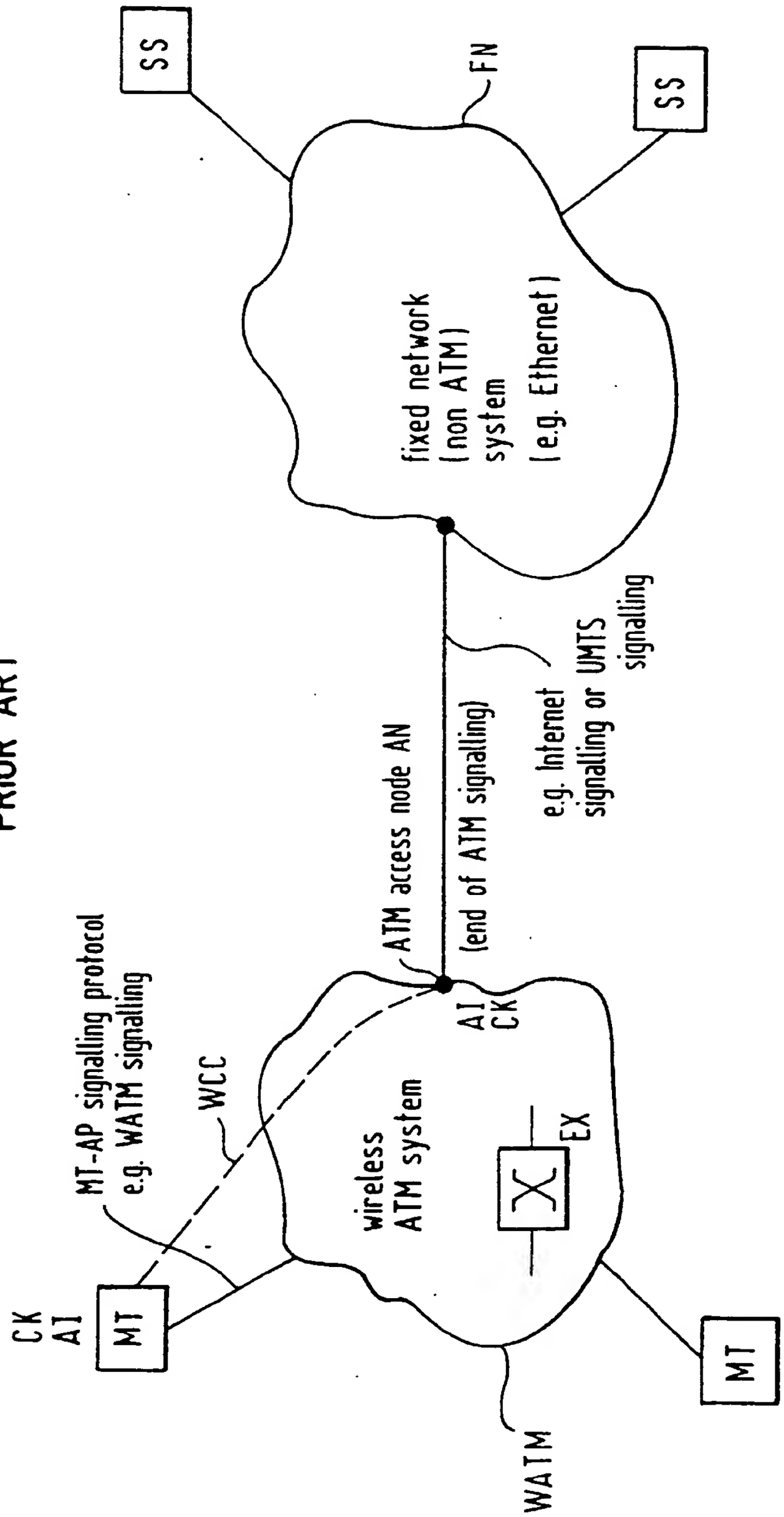


Fig. 1b
PRIOR ART

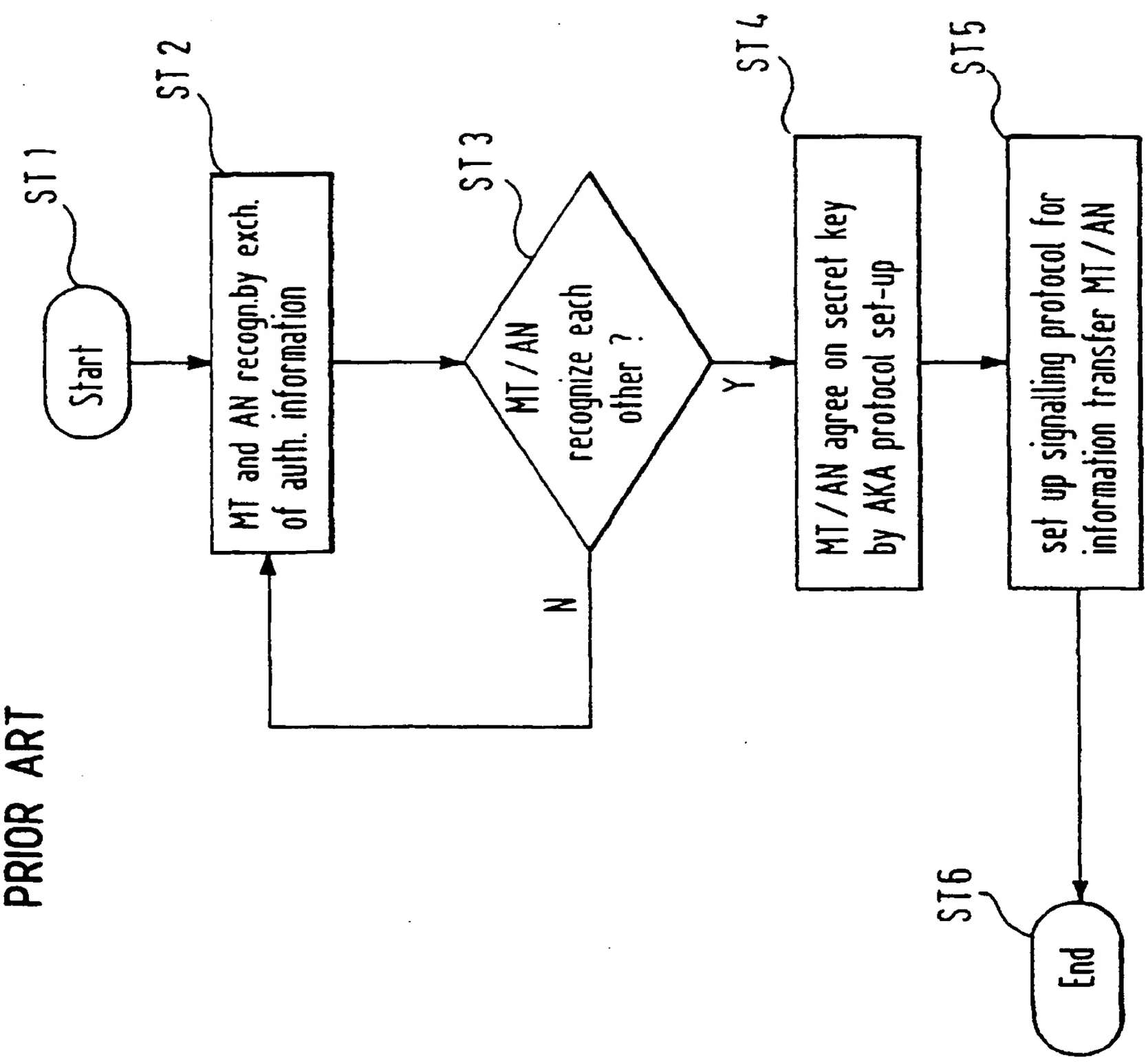


Fig. 2
PRIOR ART

Fig.3

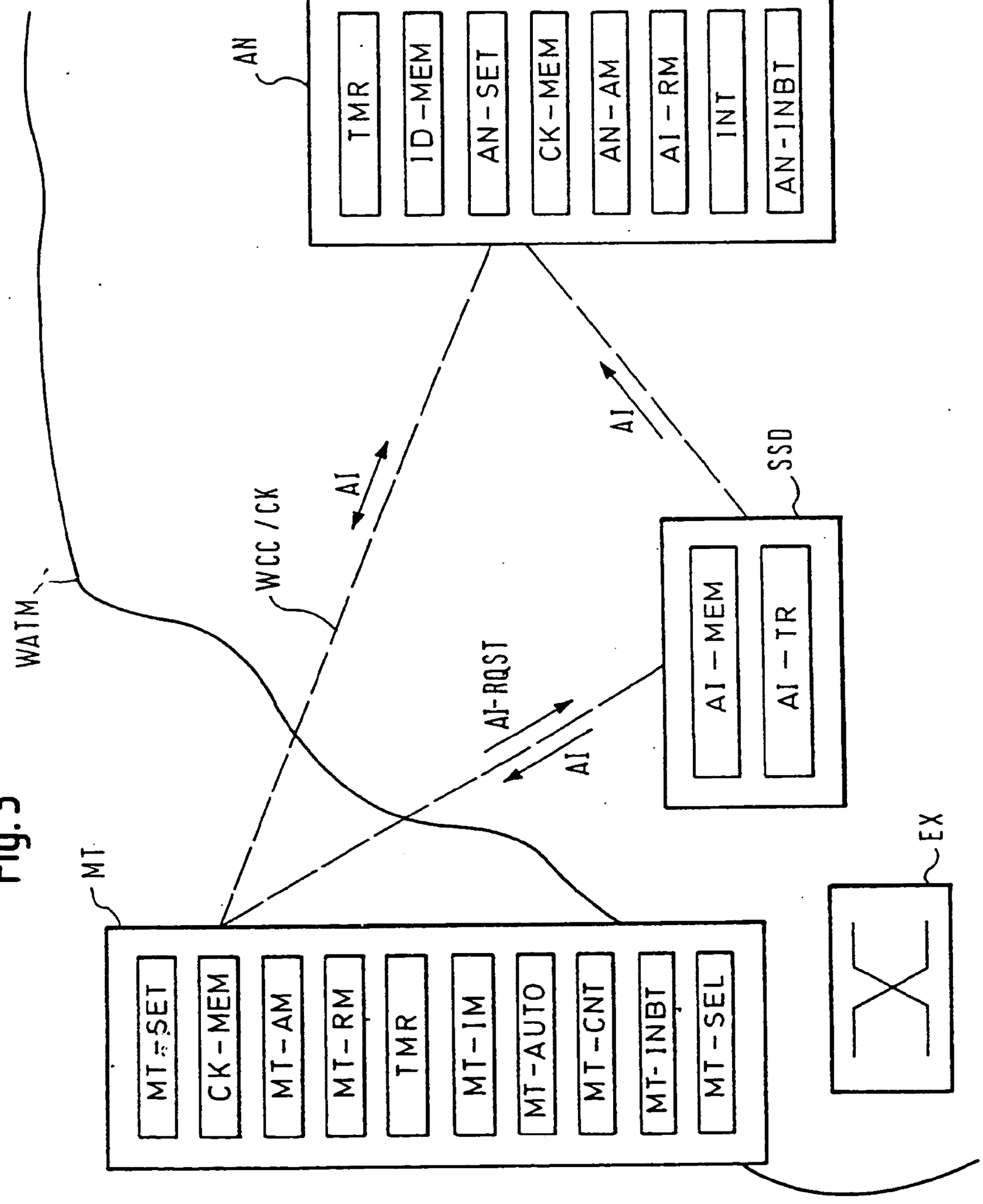

AN
TMR
ID-MEM
AN-SET
CK-MEM
AN-AM
AI-RM
INT
AN-INBT
WATM
WCC/CK
AI
AI
SSD
AI-MEM
AI-TR
AI-RQST
AI
MT
MT-SET
CK-MEM
MT-AM
MT-RM
TMR
MT-IM
MT-AUTO
MT-CNT
MT-INBT
MT-SEL
EX

Fig. 4

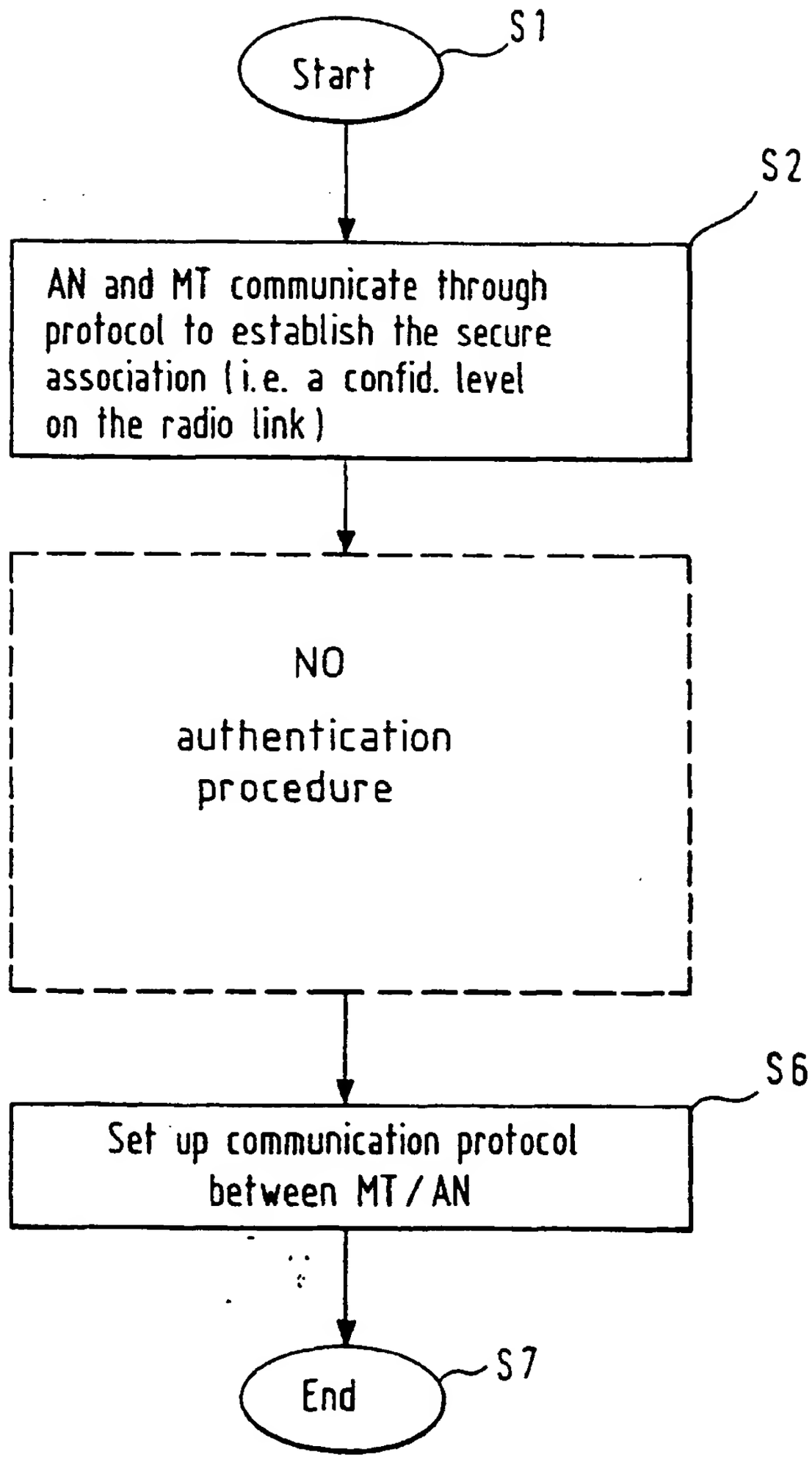
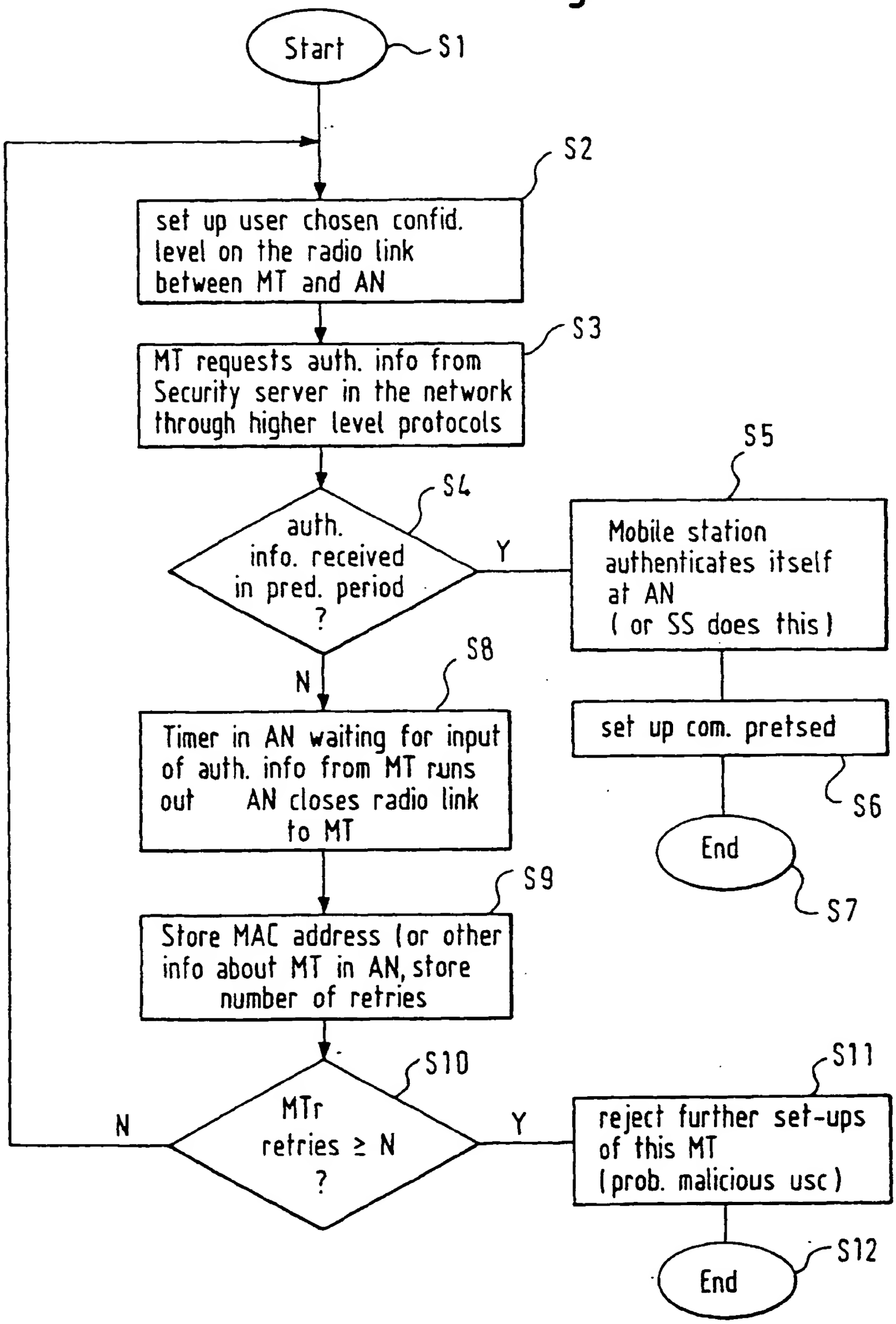


Fig. 5


Start
S1
S2
set up user chosen confid. level on the radio link between MT and AN
S3
MT requests auth. info from Security server in the network through higher level protocols
S4
auth. info. received in pred. period ?
Y
N
S5
Mobile station authenticates itself at AN (or SS does this)
set up com. pretsed
S6
End
S7
S8
Timer in AN waiting for input of auth. info from MT runs out AN closes radio link to MT
S9
Store MAC address (or other info about MT in AN, store number of retries
S10
MTr retries ≥ N ?
N
Y
S11
reject further set-ups of this MT (prob. malicious usc)
End
S12

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 3449

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 813 346 A (ASCOM TECH AG) 17 December 1997 * column 3, line 10 - line 23; figure 4 * * column 6, line 56 - column 7, line 27 *	1-38	H04Q11/00
A	EP 0 800 298 A (MOTOROLA INC) 8 October 1997 * column 4, line 27 - column 5, line 52 *	1-38	
A	US 5 539 744 A (CHU HELEN ET AL) 23 July 1996 * column 17, line 23 - line 29 * * column 30, line 23 - line 36 *	1-38	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	5 August 1998	Gregori, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Fig. 1a
PRIOR ART

: Dual Mode terminal

: Wireless Mobile ATM terminal

: Wireless ATM terminal

: Mobile ATM terminal

: Mobile ATM Switch

: Network mobility Supporting ATM Switch

: End-user Mobility Supporting ATM Switch

: ATM Switch

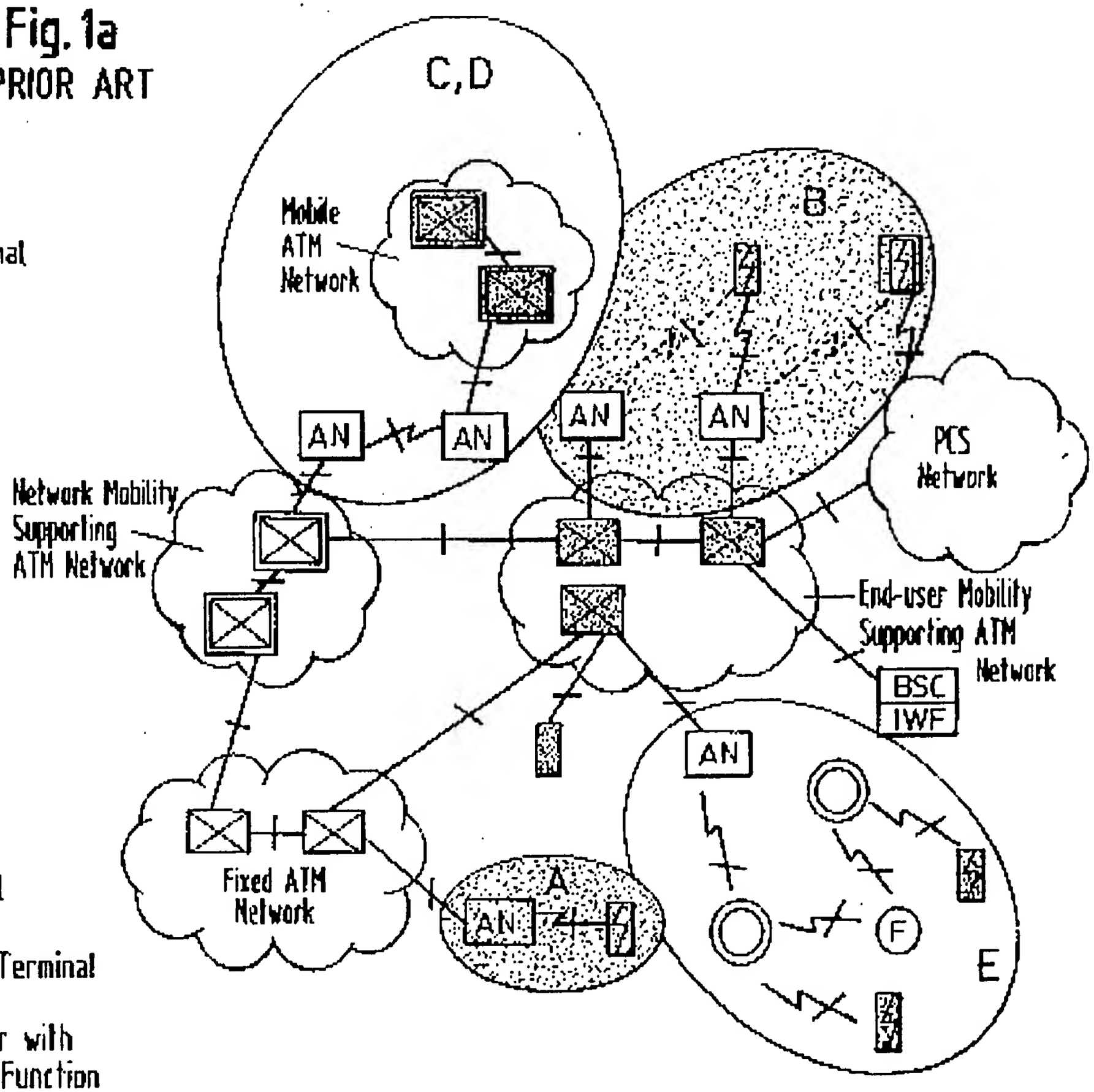
Wireless

AN : Access node

(F) : Ad Hoc Forwarding Terminal

: Ad Hoc Central Controller Terminal

BSC / IWF : PCS Base Station Controller with ATM <-> PCS Interworking Function



EP 0 939 571 A1

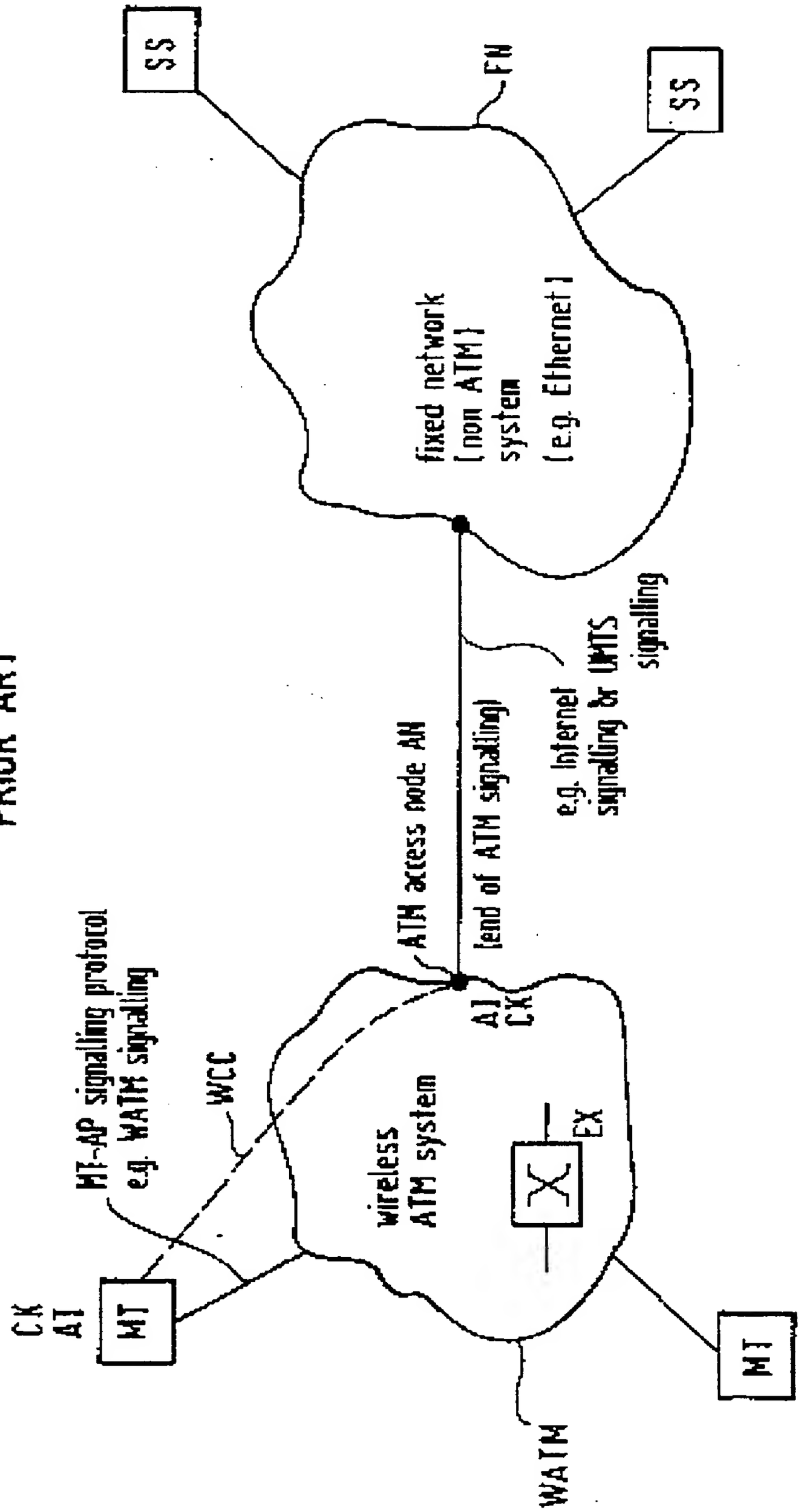


Fig. 1b
PRIOR ART

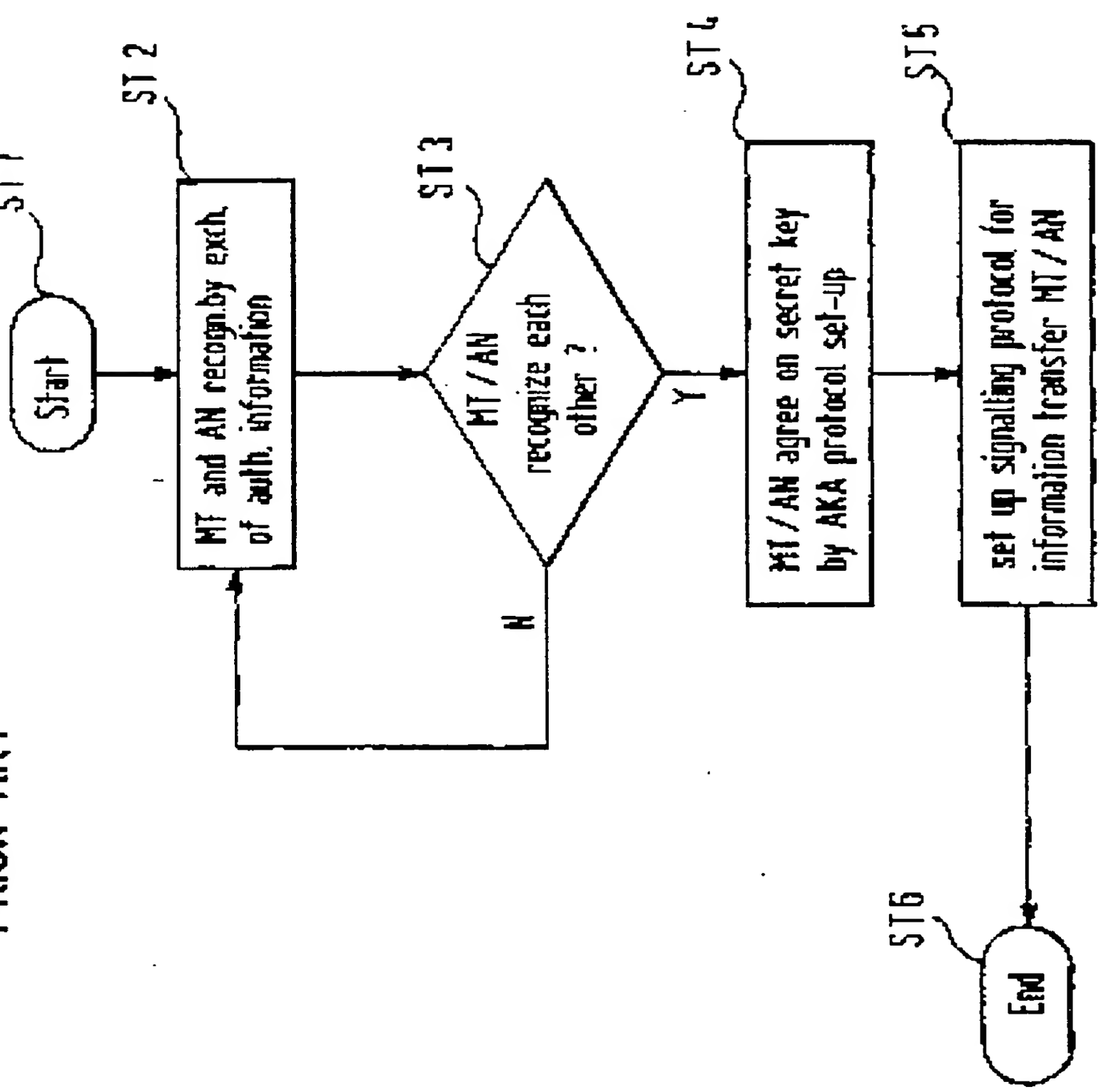


Fig. 2
PRIOR ART

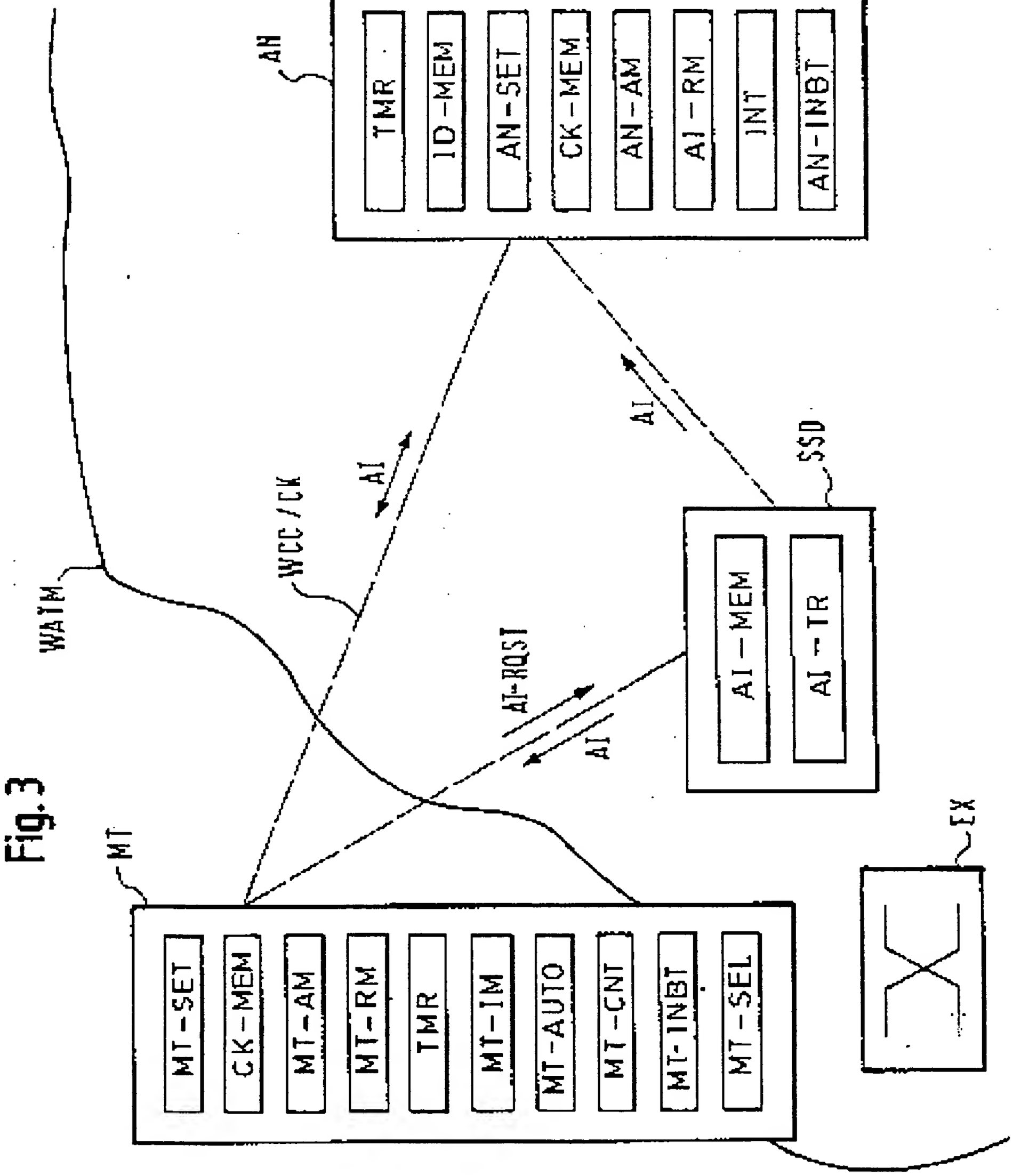


Fig. 3

Fig. 4

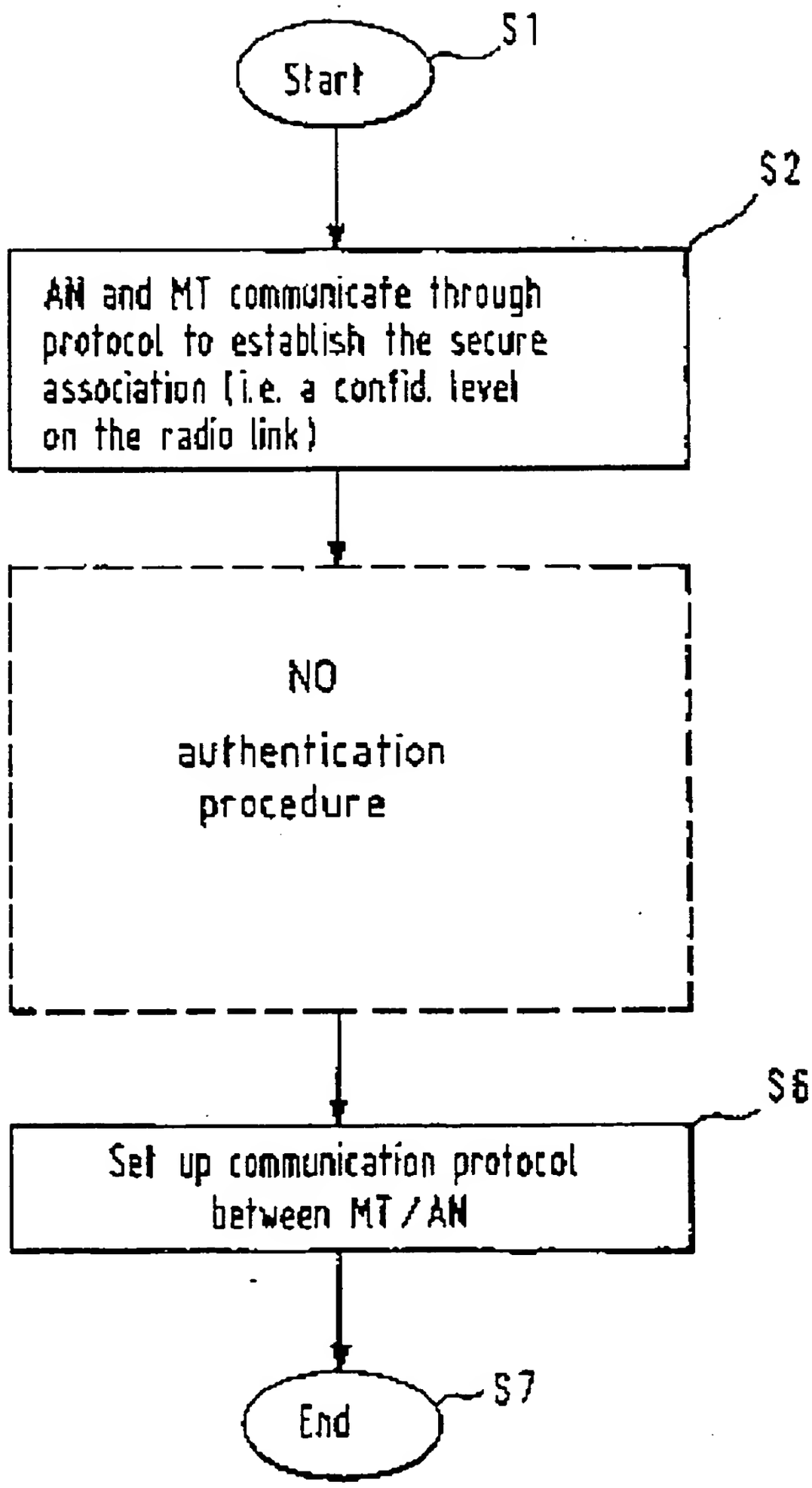
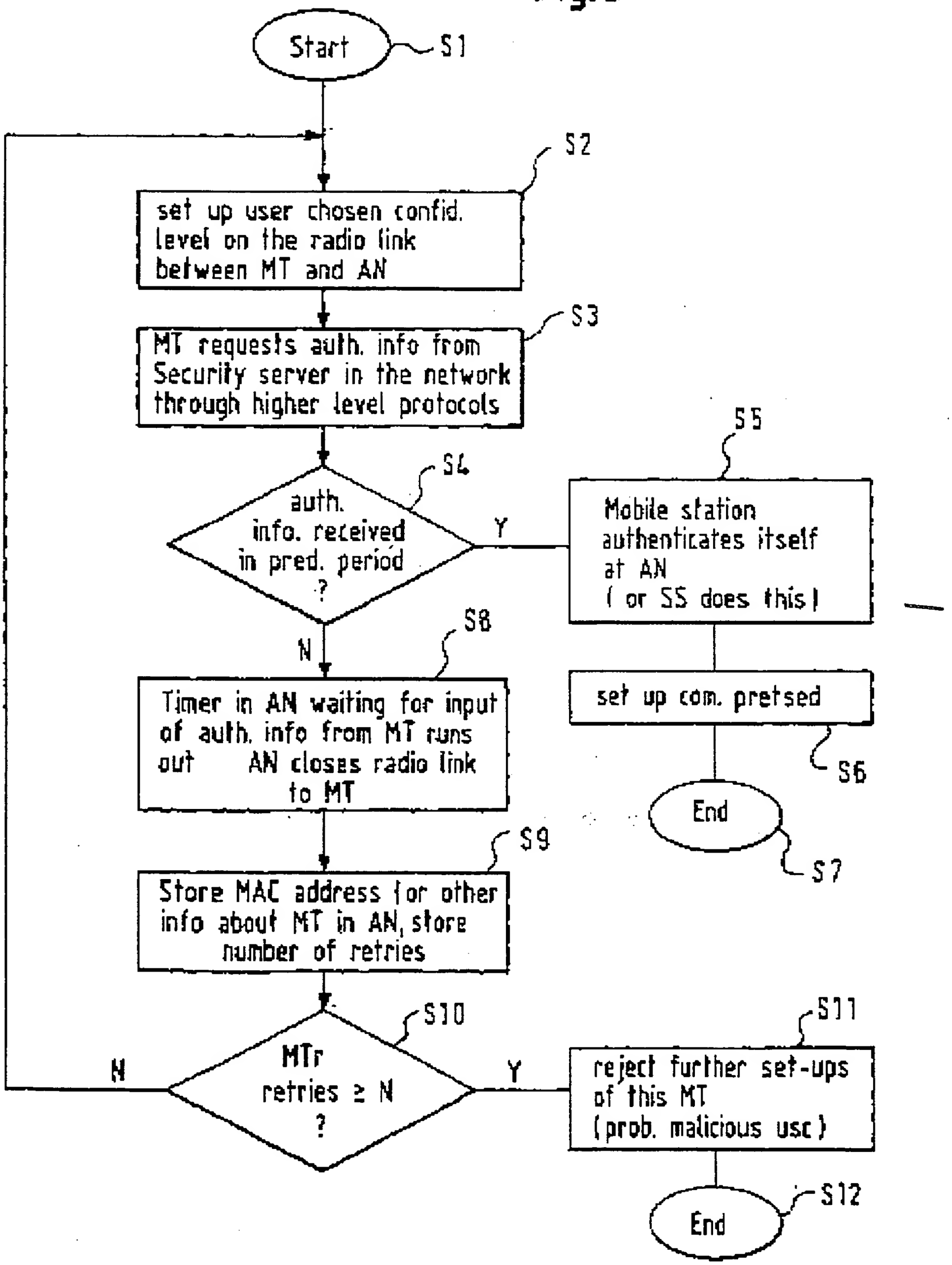


Fig. 5


Start
S1
S2
set up user chosen confid. level on the radio link between MT and AN
S3
MT requests auth. info from Security server in the network through higher level protocols
S4
auth. info. received in pred. period ?
Y
N
S5
Mobile station authenticates itself at AN (or SS does this)
set up com. pretsed
S6
End
S7
S8
Timer in AN waiting for input of auth. info from MT runs out AN closes radio link to MT
S9
Store MAC address (or other info about MT in AN, store number of retries
S10
MTr retries ≥ N ?
N
Y
S11
reject further set-ups of this MT (prob. malicious use)
S12
End